

ABSTRACT

The invention concerns a list signature method comprising: an organization phase whereby reliable authority defines parameters for implementing an anonymous electronic signature; a phase which consists in registering persons on a list of authorized members to generate a list signature, during which each person calculates a private key, and the reliable authority delivers to each person a certificate for membership of the list; a phase which consists in defining a serial number; a phase wherein a member of the list generates by means of certificate a signature containing an element common to all the signatures issued by one single member with one single serial number; a phase which consists in verifying whether the signature has been generated by a member of the list and whether the serial number has been used to generate the signature.